UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/755,450	01/13/2004	Igor Garrievich Muttik	03.047.01	1086

7590 01/05/2010

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
01/05/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/755,450
Filing Date: January 13, 2004
Appellant(s): MUTTIK, IGOR GARRIEVICH

Kevin Zilka
Reg. No. 41,429
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 19 October 2009 appealing from the Office action mailed 17 March 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct.

Appellant's brief presents arguments relating to an objection to the specification. This issue relates to petitionable subject matter under 37 CFR 1.181 and not to appealable subject matter. See MPEP § 1002 and § 1201.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

No evidence is relied upon by the examiner in the rejection of the claims under appeal.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, 55 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not disclose how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation. Furthermore, it is unclear how modified rules in one particular system has any effect on the amount of malicious traffic or the amount of propagated malware.

Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "more strongly associated" in claims 1, 18, and 35 is a relative term which renders the claims indefinite. The term "more strongly associated" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Additionally, it is unclear how modifying "said set of rules" has any effect on a set of program calls that has already been logged, or the amount of malicious network traffic and malware propagation.

(10) Response to Argument

Appellant's arguments with regard to issue #1 have not been considered because the issue relates to petitionable subject matter under 37 CFR 1.181 and not to appealable subject matter. See MPEP § 1002 and § 1201.

Appellant argues, "appellant's claimed 'determining whether said modified set of rules decreases malicious network traffic' and 'determining whether said modified set of rules slows malware propagation' … is sufficiently enabled on Page 6, lines 4-12 of appellant's specification."

Appellant's specification page 6, lines 4-12 are hereby provided:

> In determining the validity and/or quality of the secondary set it is advantageous to check if the modifications have positive effect. This can be decided either internally (by applying some higher-level rules to the set modifications) or by external signal(s). An example of such an external signal could be a report that modified rule(s) decrease the malicious network traffic or slowdown the malware propagation. As an example, after a modified set is transmitted to other computers some network sensors detect the effect (e.g., decrease of traffic) and send a "positive" signal back. That raises the score or promotes a rule from "temporary" into "permanent" set.

The test of enablement is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent couple with information known in the art without undue experimentation (MPEP 2164.01). The factors to be considered when determining whether there is sufficient evidence to support a determination that a disclosure does not satisfy the enablement requirement and whether any necessary experimentation is "undue" include, but are not limited to:

(A) The breadth of the claims;

(B) The nature of the invention;

(C) The state of the prior art;

(D) The level of one of ordinary skill;

(E) The level of predictability in the art;

(F) The amount of direction provided by the inventor;

(G) The existence of working examples; and

(H) The quantity of experimentation needed to make or use the invention based on the content of the disclosure.

Considering factor A, the claims require the use of one or more rules that are indicative of malicious computer program activity and subsequently modifying these rules. A determination is made as to whether these modified rules decreased malicious network traffic or whether these modified rules slowed malware propagation. The cited portion of the specification states that a "report" signals whether or not the modified rules successfully decreased malicious network traffic or slowed malware propagation. The specification does not detail how this report is generated and what procedures were used to generate this report. Therefore, the skilled artisan would need to perform undue experimentation to perform the above mentioned determinations because the specification fails to provide even a hint of how the report is created or how the entire network's traffic is monitored.

As stated above, the specification is silent with respect to procedures performed to create the report. Therefore, in considering factor H, the skilled artisan would need to perform a large quantity of experimentation to perform the claimed invention. The test is not merely quantitative, since a considerable amount of experimentation is permissible, if it is merely routine, or if the specification in question provides a reasonable amount of guidance with

respect to the direction in which the experimentation should proceed. *In re Wands*, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988) (citing *In re Angstadt*, 537 F.2d 489, 502-04, 190 USPQ 214, 217-19 (CCPA 1976)). In this case, the specification provides no guidance with respect to the direction in which experimentation should proceed. Additionally, monitoring an entire network's traffic for a verifiable measure of malicious traffic and propagation cannot be considered routine.

Factors E and F specify that the amount of guidance or direction needed to enable the invention is inversely related to the amount of knowledge in the state of the art as well as the predictability in the art. *In re Fisher*, 427 F.2d 833, 839, 166 USPQ 18, 24 (CCPA 1970). As stated above, Appellant's disclosure provides no guidance or direction on exactly how to make or use the invention. Therefore, the issue then becomes whether one skilled in the art can readily anticipate the effect of a change within the subject matter to which the claimed invention pertains. In the instant case, the unpredictable factors include the amount of malicious traffic and the amount of malware propagation. It is unclear how the skilled artisan would measure a change in the total amount of malicious traffic for an entire network based upon a modification of a set of rules. Likewise, it is unclear how the skilled artisan would measure a change in malware propagation based upon a modification to these same rules.

Appellant argues, "the modified set of rules may be more sensitive to additional external program calls, and may therefore be extended, resulting in more sensitive, reliable, and proactive detection, which may in turn decrease malicious network traffic and slow malware propagation."

Appellant's specification (Page 4, lines 29-32 & Page 10, line 29 – Page 11, line 6 & Figure 4) discloses that the modification of the rules involves the modification of values assigned to each program call associated with the rules. When program code is monitored for malicious behavior, a log is maintained for all program calls made by the monitored code. Each program call has a specified value assigned and when the total value of all program calls made by the monitored code exceeds a predetermined threshold, the monitored code is considered malicious. The claimed modification of the rules simply modifies these values such that the total value of all program calls made by monitored code is different from the previous set of rules. The modification of these rules has no effect on whether or not the monitored code is actually malicious. Therefore, the modification of these rules does not affect the actual amount of malicious traffic, or the actual amount of malware propagation, but instead merely modifies what the monitoring program considers to be malicious.

Appellant argues, "appellant respectfully points to Page 4, lines 9-32 of appellant's specification where it is disclosed that 'a particularly convenient way of modifying the fule set [to] make it more sensitive to the secondary set of external program calls is to increase the score values associated with such secondary sets of external program calls'…Page 9, lines 21-26 of appellant's specification discloses 'the generation of plurality of new rules which serve to more strongly associated with secondary sets of external program calls with malicious activity,' where '[t]he secondary sets themselves may not be sufficient to trigger the anti-malware response, but their score values are increased such that when they occur in combination with other detected behavioural characteristics an anti-malware response will not be

triggered'…appellant's aforementioned claim language clearly is particularly pointed out and distinctly claimed."

This argument is not persuasive because Appellant's disclosure does not provide a standard for measure the association of the claimed set of rules to malicious computer program activity. The claims require that the rules be modified such that a secondary set of program calls are "more strongly associated" with malicious computer program activity than a primary set of program calls. Appellant's specification (page 9, lines 20-29) explains that primary set of program calls is already associated with malicious activity when used to generate new/modified rules using secondary sets of program calls. Specifically, (page 9, lines 23-29) recites, "secondary sets themselves **may not be sufficient to trigger the anti-malware response**, but their score values are increased such that when they occur in combination with other detected behavioural characteristics an anti-malware response will now be triggered…it may rather be that the score values associated with a particular secondary set of external program calls is increased due to its now known association with the primary set XYZ of external program calls which is malicious." This section of the specification appears to suggest that the rules are modified such that the secondary set of program calls is associated with malicious activity to the same extent that the primary set of program calls is associated with malicious activity. Therefore, the specification does not clearly define how the modified rules that include the secondary set of program calls is "more strongly associated" to malicious activity than the primary set of program calls.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432

Conferees:

/Minh Dinh/
Primary Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432